Attachment IX

Security Summary

For

National HIV Prevention Program Monitoring & Evaluation (NHM&E)

October, 2010

TABLE OF CONTENTS

CHAPTER ONE 6

CPEMS User Interaction and Security Architecture 6

CPEMS *6*

XCPEMS and Scanning Interaction *7*

CHAPTER TWO 8

The CPEMS Security Model 8

1. CDC's Secure Data Network (SDN) *8*

2. Digital Certificate and Challenge Phrase *11*

3. Secure Sockets Layer (SSL) *13*

4. CPEMS Username and Password *15*

5. User Roles and Levels of Access *19*

6. JAVA-based Encryption *21*

CHAPTER THREE 22

Additional Security Measures for CPEMS 22

Additional Security Measures for XCPEMS 28

CHAPTER FOUR 29

Grantee Responsibilities 29

Account Management *29*

Incident Response *34*

Training *35*

Security Recommendations for Your Grantee Agency 35

GLOSSARY 42

REFERENCES 44

Suggested Citation

Centers for Disease Control and Prevention. *Security Summary for National HIV Prevention Program Monitoring and Evaluation (NHM&E).* Atlanta, Georgia: Centers for Disease Control and Prevention; September 2010

Contributors

The CPEMS team would like to offer gratitude to many contributors, including:

- Craig Thomas, Ph.D.
- Barbara Maciak, Ph. D.
- William Dolan
- Shubha Rao, MD, MPH

- # ABSTRACT

Key Objectives

The objective of this document is to inform readers about the security components of the CDC HIV Prevention Program Evaluation and Monitoring System (CPEMS). This document identifies the various components of security within CPEMS; describes details surrounding oversight of the security components of CPEMS software; briefly discusses activities related to the System Authorization (formerly known as C&A) process; explains user responsibilities regarding the use of the application; and discusses requirements for the execution of security agreements between CDC and the users of CPEMS.

Introduction

We understand that, as a CPEMS user, the privacy of client data as well as the security of that data and the application is important. This document is intended to give you that assurance.

In an effort to address security concerns shared by all users of public health applications, the federal government has established data security policies and standards that govern application security and data storage. CPEMS is compliant with these policies and standards. In order to facilitate CPEMS compliance with government policies and standards, and to protect client privacy, the CPEMS security framework incorporates the following six categories:

- System Authorization (SA) resulting in an Authorization to Operate (ATO)
- Identification and monitoring of the security components of CPEMS
- Examination of security issues and events related to CPEMS
- Documentation of software/hardware security assessments
- Involvement of a CDC-appointed security steward
- Execution of security agreements between CDC and the CPEMS users

CPEMS agencies can contribute to the security of CPEMS by:

- Acknowledging and fulfilling agency responsibilities
- Implementing the security recommendations
- Maintaining agreements with system users which protect the system and your data

Acronym Definitions

Please refer to the following table for acronyms used within this document.

Acronym	Term
ATO	Authorization to Operate
SA	System Authorization
CBO	Community-Based Organization
CDC	Centers for Disease Control and Prevention
CCPEMS	Centralized CPEMS
CT	Counseling and Testing
DHAP	Division of HIV/AIDS Prevention
FIPS	Federal Information Processing System
GUI	Graphical User Interface
HHS	Department of Health and Human Services
IRMO	Information Resources Management Office
ISSO	Information System Security Officer
ITSO	Information Technology Services Office
JRE	JAVA Runtime Environment
MOU/MOA	Memorandum of Understanding/Agreement
NIST	National Institute ofStandards and Technology
OCISO	Office of the Chief Information Security Officer
CPEMS	HIV Prevention Program Evaluation and Monitoring System
ROB	Rules of Behavior
SDA	Self Decrypting Archive
SDN	Secure Data Network
SSL	Secure Sockets Layer
SLA	System Level Agreement
SRA	Security Risk Assessment
XPEMS	External PEMS

CHAPTER ONE

CPEMS User Interaction and Security Architecture

CPEMS is deployed in two different ways; therefore, the security system diagrams vary depending on whether you are a Centralized PEMS (CPEMS) or External PEMS (XPEMS) user. The following diagrams show how users interact with the different systems and the security architecture for each.

CPEMS

CPEMS is a centralized web-based solution consisting of a web server, application server and a database server that reside on the CDC network. Users process data through the CPEMS web interface, interacting with CPEMS through a series of screens, progressing from the welcome page to completion through a series of data gathering screens.

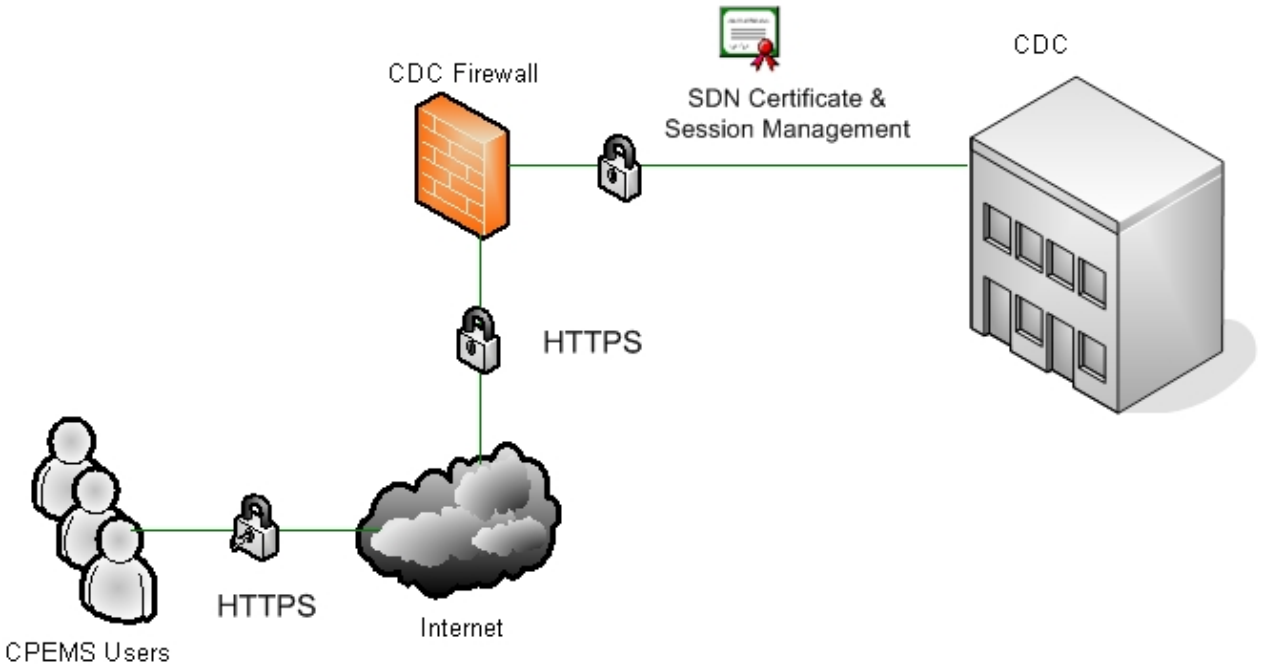


Figure 1: CPEMS Interaction and Encryption

XPEMS and Scanning Interaction

XPEMS is an external solution for grantees who prefer not to, or who are unable to support the technology required to migrate to other CPEMS solutions. XPEMS users collect information requested by the CDC, process the data locally, convert the data into a format that complies with the CPEMS application, and transfer the requested data using the CDC Secure Data Network (SDN). This system serves as a secure medium of communication to transport data sent via CPEMS and scanning servers.

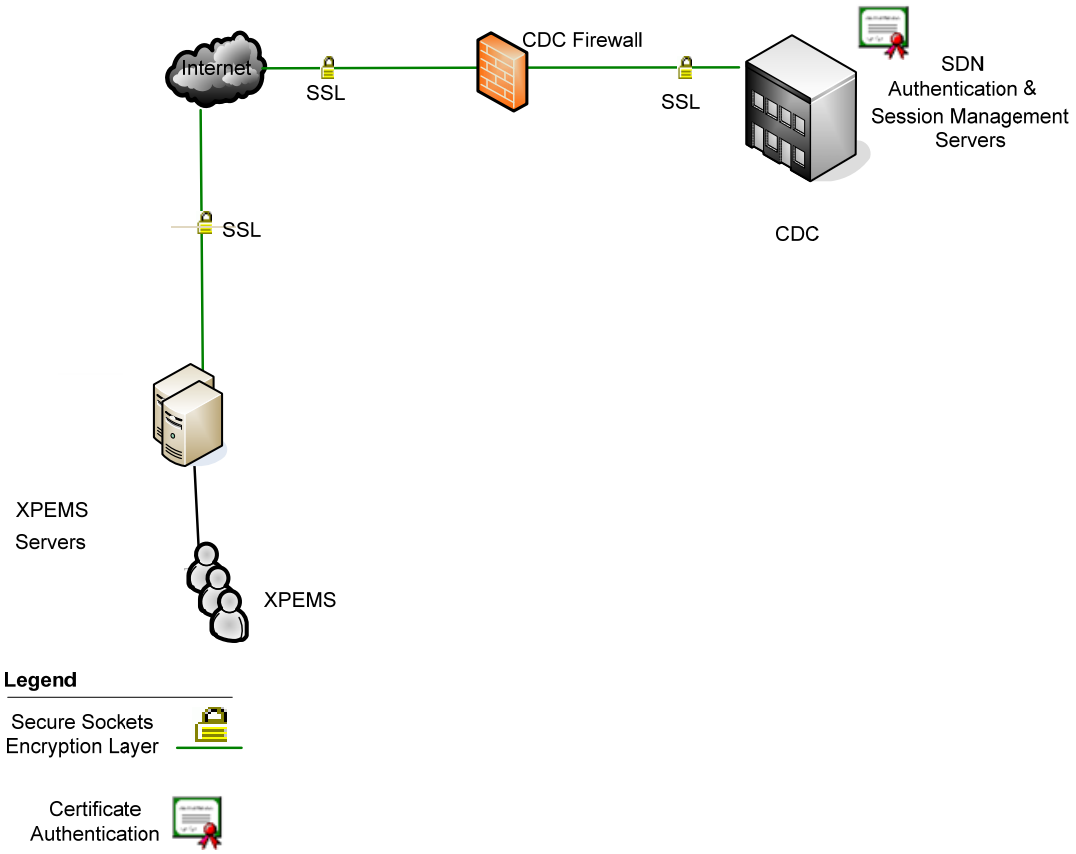


Figure 2: XPEMS and CT Scanning Interaction and Encryption

CHAPTER TWO

The CPEMS Security Model

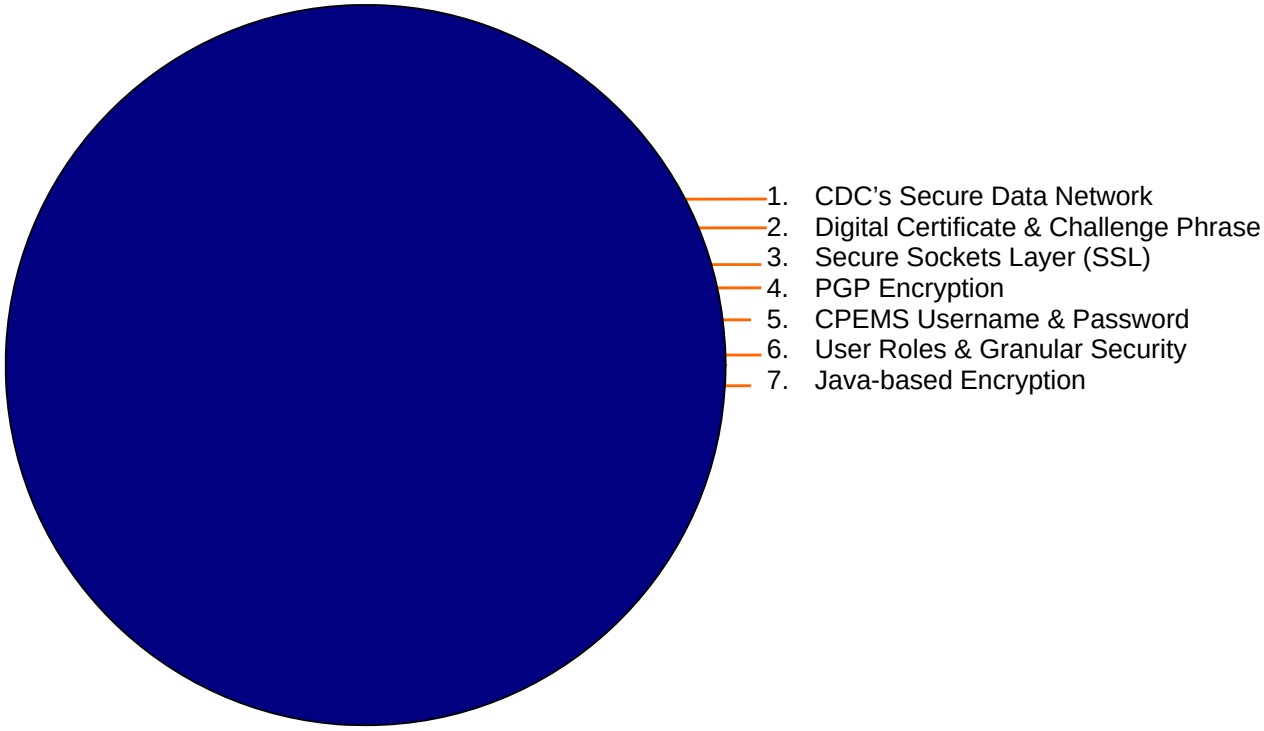


Figure 3: Layered Security Model

The diagram above shows the CPEMS security model. Each layer performs a different function and all layers, together, protect client data. Moving from the outside of the diagram to the inside, each layer will be explained.

1. CDC's Secure Data Network (SDN)

The security components of CPEMS associated with the SDN are described below.

Session Management

The SDN provides session management capabilities using specific software. The software provides CDC with a centralized security infrastructure for managing user authentication and access to Web applications. When users leave their computers unattended while logged into CPEMS, unauthorized individuals could use the system, potentially exposing confidential information. One of the important policy-based controls enforced by the software helps mitigate this risk. Within the SDN, the idle timeout is set to 15 minutes. Therefore, sessions

where no activity[1] takes place for 15 minutes are terminated, and further system activity is prevented (until another login occurs).

Intrusion Detection

Most enterprise firewalls act as filters to determine which traffic can enter a network and which cannot. While the firewall examines incoming traffic, it does so only to prevent unauthorized traffic from entering the network; it does not look at the intent of the traffic. If traffic arrives from a single address on each port, the firewall will allow the authorized traffic (blocking the rest), but it may not recognize that this traffic pattern is consistent with port scanning—often the first step in an attack. Intrusion detection software, on the other hand, is designed to recognize unusual traffic patterns and respond, typically alerting administrators and allowing them to take corrective action.

The SDN uses intrusion detection software. This software provides Web intrusion prevention against application-level breaches by identifying legitimate requests and permitting only those actions to take place. By preventing breaches and subsequently alerting administrators to any type of application manipulation through the browser, expected application behavior is maintained.

Vulnerability Testing

Examples of various problems have surfaced due to exploits of information technology – both hardware and software. In order to protect against these attacks, two types of vulnerability assessment are performed on the CPEMS infrastructure:

- Server Vulnerability Testing
- Application Vulnerability Testing

Server Vulnerability Testing

This type of testing focuses on uncovering weaknesses in the configuration of the server software. In order to perform server vulnerability testing, various security analysis tools arerun on all servers supporting CPEMS to scan for common system configuration issues, and identify missing security updates.

Application Vulnerability Testing

Often known as buffer overflow attacks, application vulnerabilities have cost businesses and personal users billions of dollars. One step in preventing these attacks is pre-deployment application vulnerability testing. CPEMS is scanned prior to any deployment in a production environment using the latest known vulnerability tests. In the event any weaknesses are discovered, they are mitigated and rescanned until no vulnerabilities remain. Within the CDC, the SDN provides application vulnerability testing as well as the Security Steward using

[1] Within the context of Web applications, the phrase “no activity” means no activity between the Web server and the Web browser. If users are sitting at their PCs entering data on a Web form, no information is flowing to the server. Therefore, if a user requires 20 minutes to complete a Web form, the session will expire and the user will be required to log in again before saving the form.

specific software. As part of the CDC change management process, CPEMS undergoes vulnerability scans any time a change or update is made to ensure no new vulnerabilities are introduced into the software. This software program detects security vulnerabilities automatically as an integrated component of an enterprise security process review.

2. Digital Certificate and Challenge Phrase

CPEMS uses two levels of authentication.

- First, a digital certificate and challenge phrase is used to validate users before providing access to the SDN. After validation, access is granted to CPEMS activity and role assignments.
- Second, CPEMS requires users to enter a unique username and password in order to log in to the application.

In order for offenders to circumvent these security mechanisms, they would have to possess a valid digital certificate for which they knew the associated challenge phrase and discover a valid username and password combination for the CPEMS application.

The following figure depicts the system login and permission assignment process.

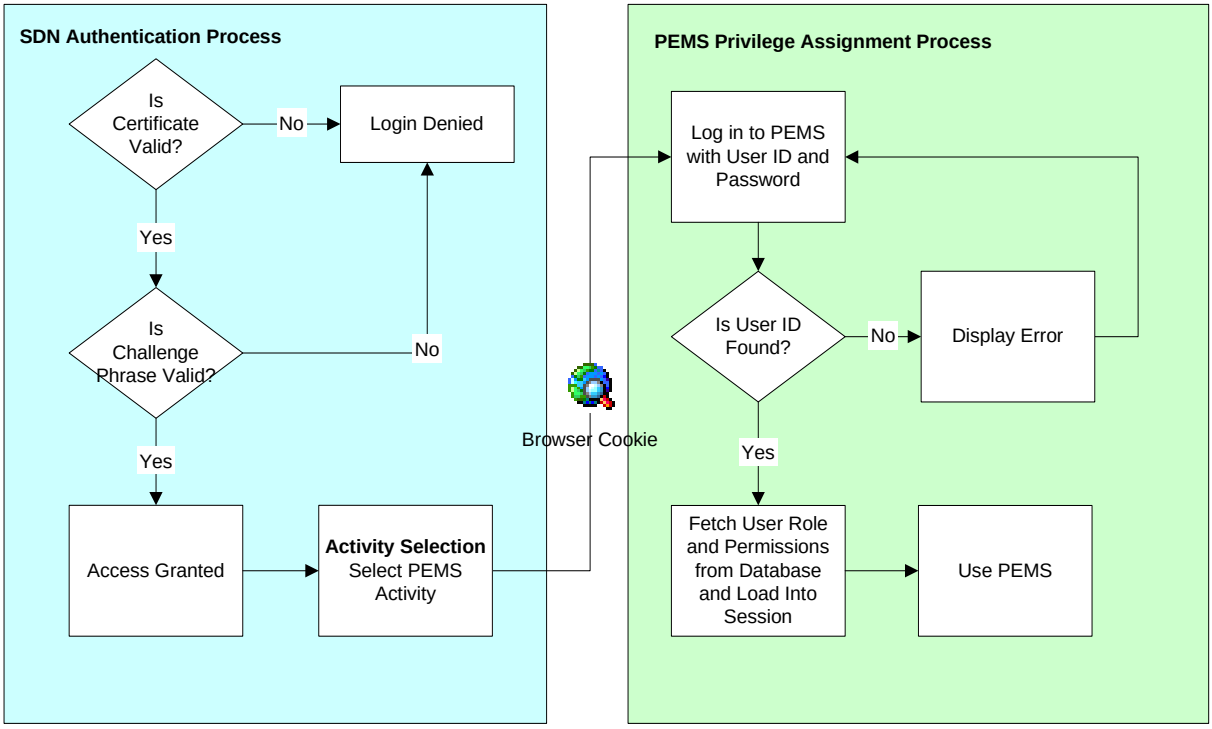


Figure 4: CPEMS Login and Permission Assignment Process

To guarantee maximum security, digital certificates should not be put on hand-held, or laptop computers.

In addition, if a person leaves an organization, that digital certificate should be removed (de-activated) and a new one should be installed by the new user. Contact your CPEMS Agency System Administrator, as defined in Chapter Two, Section 5 (page 18.) Certificates expire yearly and therefore each user must apply for a new digital certificate each year.

When signing in to the Secure Data Network (SDN), the first screen that users encounter is the screen below. In order to successfully log in, users must supply the challenge phrase which they established when applying for their digital certificate.

NOTE: The notice displayed is required on all government systems and refers to the fact that administrative and security personnel have access to the SYSTEM, not the DATA. Your client data are protected as described elsewhere in this document.

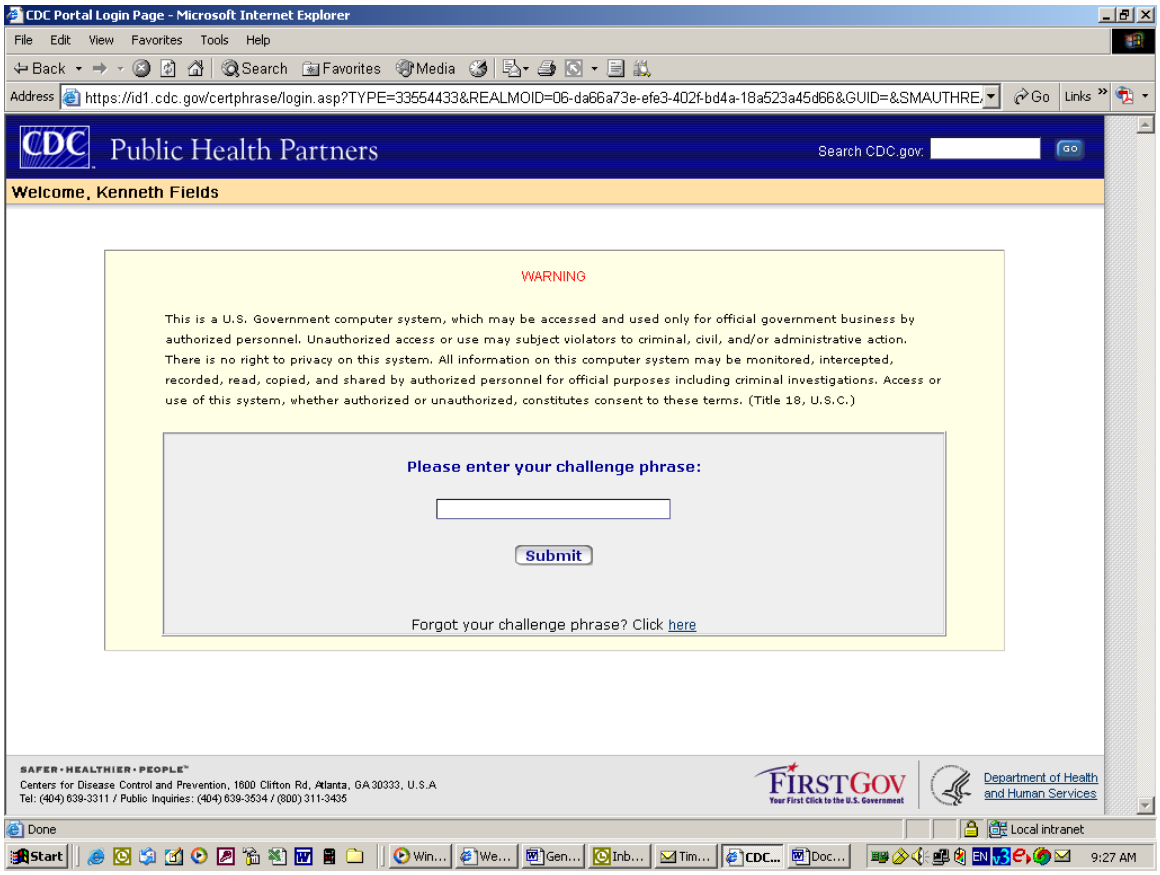


Figure 5: SDN Challenge Phrase Screen

3. Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) provides encryption throughout the system. Connections are secured by SSL between the client's Web browser and the Web server within the SDN. Additional SSL connections secure message traffic between (1) the Web server and the application server, and (2) the application server and the database servers.

The CPEMS application uses Secure Sockets Layer (SSL) between web-browser clients and the web server that accepts data from users. Additional SSL sessions secure data between the web server and the application server, and the application server and the database server. Each of these SSL sessions uses the same type of encryption used by all major financial services and electronic commerce sites today. From a user's perspective, then, confidential information is encrypted from the time it leaves the PC to the time it is stored in the central database.

CPEMS also supports persistent encryption of specific data variables (identified as sensitive by the CDC) using the 3DES algorithm. This algorithm is also known as Triple DES, employs a 168-bit encryption key and is FIPS 140-2 compliant. Thus, in addition to being encrypted with SSL during transit, some information remains encrypted within the database, visible only to the agency that entered it. The system encrypts client-identifying variables and includes (in the online help) an encryption indicator for each variable. The online help also includes a warning to users that information entered in non-identifying data fields will not be encrypted. The following is a list of variables that will be encrypted in CPEMS:

Client Information	Partner Information
G105 - Last Name	PCR203 - Last Name
G106 - First Name	PCR204 - First Name
G107 - Middle Initial	PCR205 - Middle Initial
G108 - Nick Name	PCR206 - Nickname
G109 - Aliases	
G110 - Date of Birth-Month	PCR210 - Date of Birth-Month
G111 - Date of Birth-Day	PCR211 - Date of Birth-Day
G125 - Physical Description	PCR219 - Physical Description
G128 - Address Type	PCR220 - Address Type
G129 - Client Street Address 1	PCR221 - Street Address 1
G130 - Client Street Address 2	PCR222 - Street Address 2
G131 - Client City	PCR223 - City
G132 - Client County	
G133 - Client State	PCR224 - State
G134 - Client Zip Code	PCR225 - Zip Code
G135 - Client Phone Number (Day)	PCR226 - Phone Number (Day)
G136 - Client Phone Number (Evening)	PCR227 - Phone Number (Evening)
G137 - Primary Occupation	PCR228 - Primary Occupation
G138 - Employer	PCR229 – Employer
G139 - Notes	Notes

Searching Encrypted Data

An important feature of the application is the ability to search encrypted fields, (such as a first name) in order to locate a client. There are certain restrictions regarding the ability to search the database: encrypted data does not allow LIKE searches that are typically performed to implement these searches. To ensure a quality user experience, the system allows certain wildcard searches with restrictions. A restricted search allows users to search up to the first four characters of a last name, or the entire name, but not the first five characters. In order to perform these searches, CPEMS implements a one-way division of the first one, two three and four characters of the last name of all client entries in the system. These partial last name divisions are stored in a separate column in the CPEMS database. When a CPEMS user executes a search request for the last four letters of a last name, the system will generate a one-way division from the user input and compare it to the information stored in the separate column in the CPEMS database. The system works similarly if users search for the first letter, first two letters or first three letters of a name. This partial-matching solution allows for some flexibility in user searches while at the same time supporting encrypted identifying data and efficient search algorithms.

4. CPEMS Username and Password

Prior to accessing CPEMS with a username and password, the SDN authentication (digital certificate / challenge phrase validation) and CPEMS activity selection must be complete. CPEMS uses role-based access in which user accounts with roles and permissions are set up, usernames are assigned, and a means of authenticating users, such as passwords, is provided. In order to successfully log in to CPEMS, a user must supply a valid username and password, and agree to the conditions displayed in the pop-up message box, shown below. Users logging in to CPEMS for the first time are required to change their password upon first entry to the system.

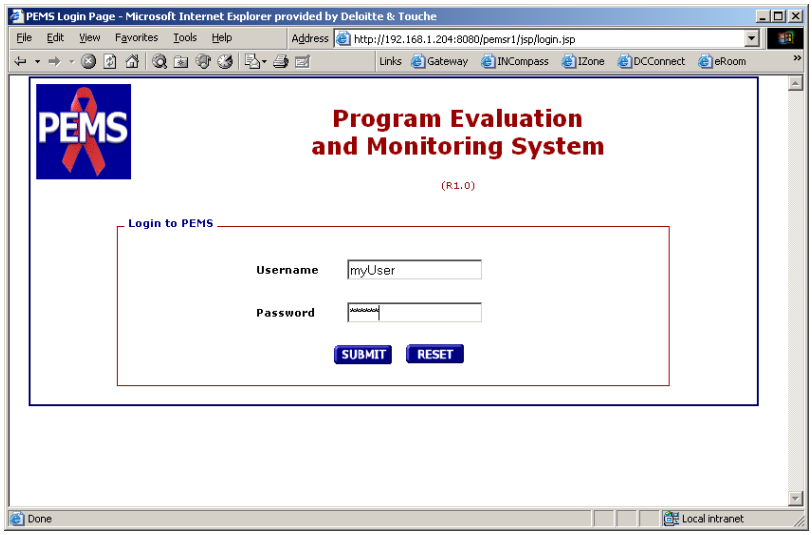
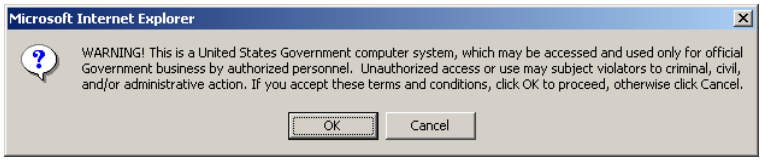


Figure 6: CPEMS Login Page



For the sake of clarity, the text of the message is displayed to the right of the figure.

Figure 7: Conditions of Use

WARNING! This is a United States Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use may subject violators to criminal, civil, and/or administrative action. If you accept these terms and conditions, click OK to proceed, otherwise click Cancel.

The following table provides details regarding user passwords.

Topic	Details
Password complexity	The password must: Be 8 characters or longer Contain three of the following four classes: a-z A-Z 0-9 !,@,#,$,%,^,&,*,(,),-,_,=,+, etc. Not contain the user's given name, surname, or system username
Password changes	Users must be able to change passwords in their system.
Password loss	Administrators may reset/change your user passwords.

Passwords should be known only to the individual user**. Do not leave passwords written on a "sticky note" on the desk or wall.** No expiration date is automatically set for CPEMS passwords. Users should change their password every 90 days.

If a user's employment is terminated at an agency, the passwords should be de-activated and the Agency System Administrator should be notified.

Disable Browser Password Caching

In addition to changing passwords on a regular basis, the function in Windows that "remembers" or stores a password so that the password does not have to be entered each time the user logs in should be disabled. To disable this option, open a new Web browser, and select Internet Options from the Tools menu.

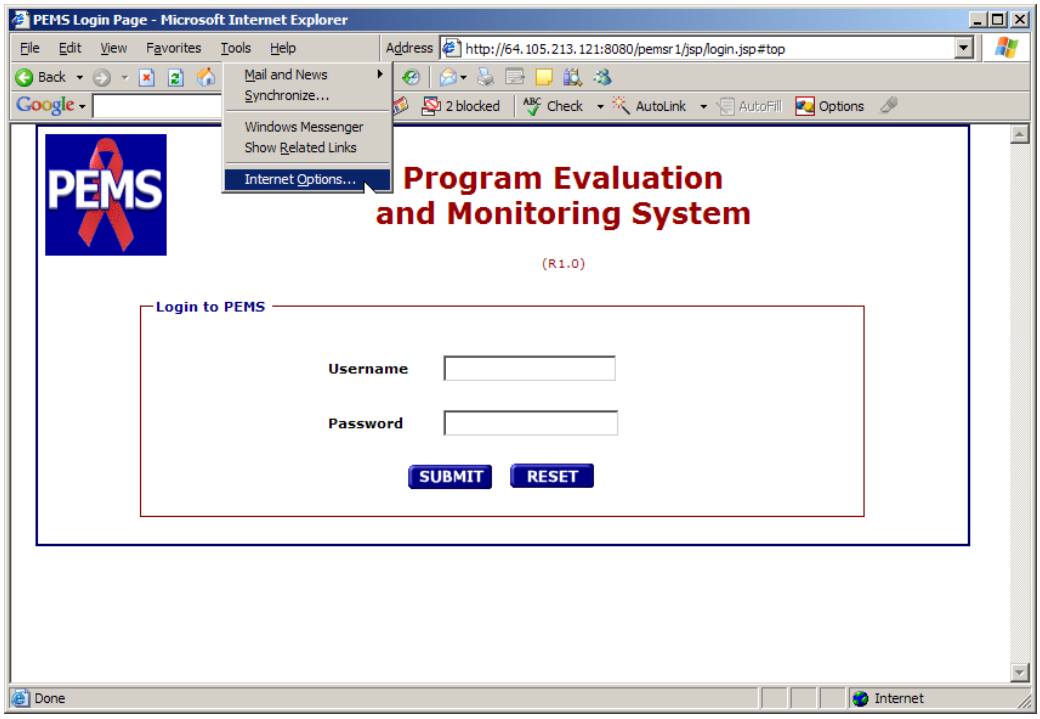


Figure 8: CPEMS Login Page

The Internet Options window displays. Switch to the Content tab, and click the AutoComplete button.

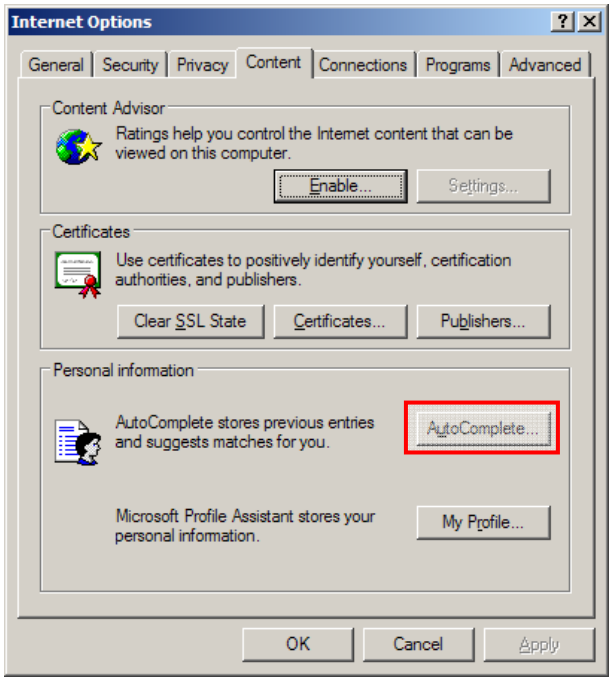


Figure 9: Internet Options Window

The AutoComplete Settings window displays. While some of the settings in the 'Use AutoComplete for' frame may have been disabled by your Agency System Administrator, you should ensure that only Web addresses remains checked (i.e., clear the checkmark from the other boxes).

Finally, click the Clear Forms and Clear Passwords buttons.
Note: *Clicking these buttons will erase any form and password information your browser has cached for you, so make sure you remember your credentials before you perform this step.*

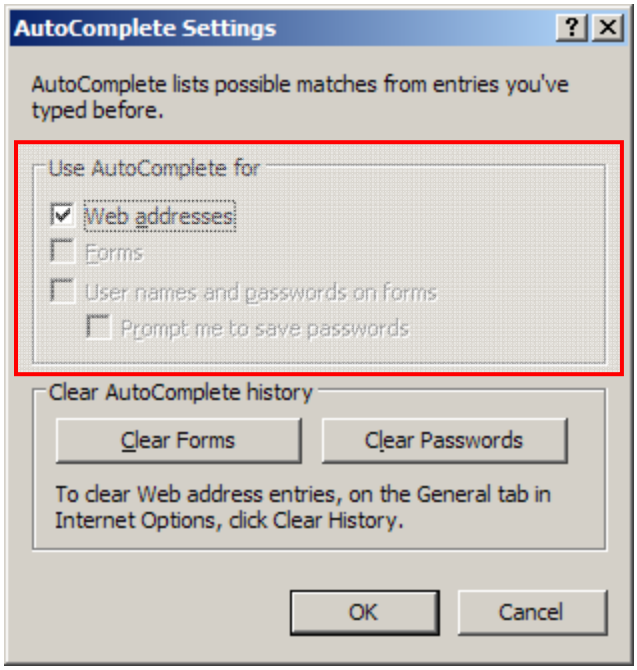


Figure 10: AutoComplete Settings Window

5. User Roles and Levels of Access

In addition to requiring users to obtain certificates and create challenge phrases and passwords, selecting responsible individuals for various activities associated with the operation and use of CPEMS is also required. CDC has designated its responsible parties. Each agency is also required to designate a CPEMS Administrator as the overall responsible party for CPEMS operations and assigning user roles.

Users of CPEMS are only able to access:

1. The data that they enter
2. The data that belongs to their individual organization
3. Specific data to which they have been given rights

Access of other grantee organizations is restricted. Users are treated as having no privileges if not specifically granted a privilege. The responsibility to grant and restrict access is given to the CPEMS Agency System Administrator.

The four access privileges available to be given to CPEMS users are:

1. View – This level allows users to view data (in read-only format).
2. Add/Edit – This level allows users to add new data and modify existing data (they are also permitted to view data).
3. Delete – This level allows users to delete data (they are also allowed to add/edit and view data).
4. Manage – This level is for CPEMS administrators only.

Following is a list of core CPEMS roles. At health departments and/or at directly or indirectly funded CBO's, all or some of these roles may be the responsibility of a single person.

- CPEMS Super System Administrator
- CPEMS Agency System Administrator
- Agency Budget Role
- Agency Information Role
- Aggregate Health Communication/Public Information (HCPI)
- Aggregate Health Education Risk Reduction/Outreach (HERR/OR)
- Aggregate Service
- Client Service
- Community Planning Data Role
- Counseling and Testing (CT)
- Data Transfer Role
- Partner Counseling and Referral Services (PCRS)
- Prevention Case Management (PCM)
- Program Budget Information Role
- Program Information Role
- QA Reports and Client HERR Role

- Worker Reports Role (user defined)

The user roles allow access only to particular screens and prevent access to other screens. In order for a user to obtain access to CPEMS, the following steps must occur:

1. A CPEMS Agency System Administrator sends a letter to the CDC requesting access to CPEMS for a set of users.
2. The designated set of users is invited to apply for digital certificates.
3. Digital certificates are granted access to the CPEMS Software activity within the SDN.
4. A CPEMS Agency System Administrator signs in to CCPEMS and creates accounts for designated users.
5. A CPEMS Agency System Administrator assigns new users to existing core roles.
6. A CPEMS Agency System Administrator may create new roles to remove privileges associated with core roles and assign users to those roles (in order to further restrict access).
7. Designated users (of the grantee) log in to CPEMS and the application security component determines which set of roles apply.

6. JAVA-based Encryption

CPEMS includes JAVA-based encryption (168-bit, 3DES high level encryption). In addition to this, data is transported at all times using SSL encryption. This is called double-layer encryption. We will supply the encryption application necessary for the transmission of data in the required format. CPEMS users should use this application to encrypt the data in a manner that will only allow someone with the appropriate "key" to unlock the data. The CDC DHAP/IT Help Desk can provide assistance with encryption issues.

Encrypted data can only be UN-encrypted if four conditions exist:

- The data must be UN-encrypted at the site where it was entered; no other site would have the algorithms
- The user must have a valid certificate and know the challenge phrase
- The user must know the password for that certificate
- The user must have been given permission by the Agency System Administrator to access these particular data.

CHAPTER THREE

Additional Security Measures for CPEMS

CPEMS is a part of the CDC System Enterprise Architecture and is held to a high standard of performance with regard to security. The following standards areapplied to CPEMS.

Standards Required by Law for Federal Systems

- Clinger Cohen Act of 1996 (Public Law 104-106)
- OMB Budget Circular A-130
- Federal Information Security Management Act (FISMA)
- E-Government Act of 2002
- HHS Information Security Program Policy
- Executive Orders, Directives, Regulations, Publications, Guidance(s)
- National Institute of Standards and Technology Special Publications 800 Series

Compliance Requirements Include filing/signing documents

- System Authorizationprocess
- CDC Capitol Planning Investment Control (CPIC) OMB reporting
- Enterprise Systems Catalogue
- Complete ongoing processes regularly
- Various service agreements that must be executed

System Authorization

All federal information systems must receive a System Authorization (SA). CPEMS successfully completed this process and was given an Authority to Operate (ATO) until 11/18/2012. CDC has moved to a new enterprise-wide C&A process, supplemented by specific controls and tests for each application.

System Auditing

CPEMS supports auditing of the activity and interactions of the users. Through the application, each record is marked with the following fields:

- Who created
- Date created
- Who updated
- Date updated

Storing this information allows administrators to identify which user entered or modified system data, thus permitting them to associate changes with a given user. These basic auditing features have been included since program inception (i.e., since CPEMS R1.0).

Programmatic Tracking

CPEMS also provides auditing for particular variables using a capability referred to as Programmatic Tracking. This new functionality allows users to create new records, and append updated records to a data set without overwriting previously entered records. Where appropriate, the system also allows users to create updated records based on previously entered data. The following client-level data sets shall support programmatic tracking:

- Client Demographics and Locating Information
- Risk Profile Data and Detailed Behavior
- Confirmed HIV Status

The above data sets are captured and then ordered based on the date collected field. The system tracks updates to client demographic information by storing the most recently collected data record in one table and storing all previously collected data records in a separate history table. This table structure allows the system to perform faster searches on client demographic information – an important characteristic given the frequency of client searches. History for Risk Profile, Detailed Behaviors and Confirmed HIV Status data is maintained in the same table as the most current record. The divergent approaches are related to system behavior; Risk Profile and Confirmed HIV Status data are always accessed for a specific client. Thus, storing current and historic records in the same table allows for faster, more efficient access to a complete overview of a client.

In addition to allowing access to updated records, the system also allows users to view and edit previously entered data. It is important to note the distinction between record updates and record modifications (referred to as Edits in the system). *Record updates* represent the creation of a new record in order to track the evolution of some characteristic over a period of time, whereas *record modifications* represent the correction of incorrect data. As an example, consider a provider collecting information on one of their clients. For the first visit, the provider documents the name of the pregnancy test given and that the client is not pregnant. The next year, the client has a follow-up visit and the provider documents the name of the pregnancy test given and that she is now pregnant. Individually, each entry represents a snapshot of the client's pregnancy status at a distinct point in time. The second entry represents an update to the record. Now consider the provider is later reviewing the information collected for the client. The doctor notices that the name of the test given in the first visit was misspelled on the documentation. The doctor corrects the name of the test and overwrites the first entry. This represents a modification to the record. Programmatic tracking will not provide a history of record modifications. As with any system record, if the user performs an edit, the system will replace the old version with the new and update the last modified date.

Beyond the audit captured by CPEMS, the systems upon which CPEMS relies, namely the SDN and Chamblee campus data center, provide various auditing on each tier of the system: the authentication system (digital certificates), the web server, the application server and the database server.

CPEMS Database Back-up Procedure

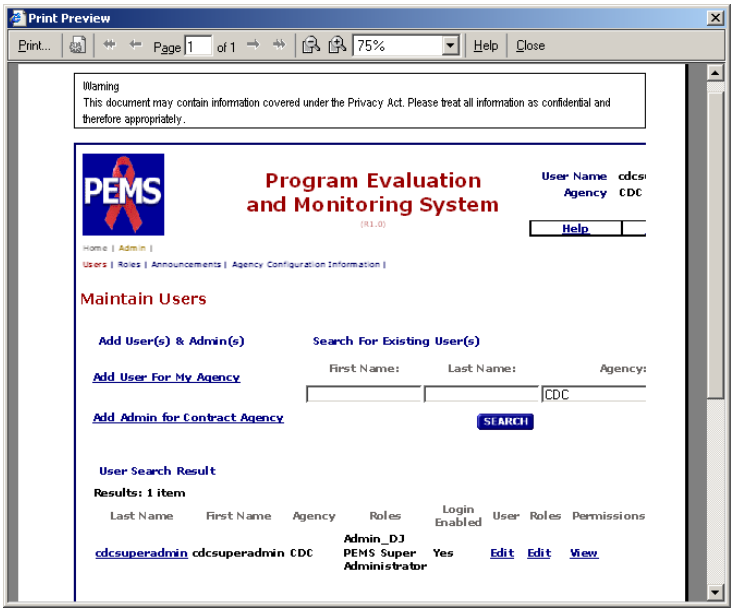
1. A full back-up of the CPEMS databases (staging, training, productions support, production) is performed daily
2. The SQL back-ups are copied to the SAN, where they are stored for one month.
3. They are then backed-up on physical tapes, which are kept in the tape library system (StorageTek L700E).
4. Once backed-up, the tapes are then moved off-site to a remote facility and archived. They are stored at off-site remote facility for three months and then are reused.
5. In the event of a disaster or data center failure, back-up tapes could be sent by overnight express.

CPEMS Application Server (SDN) Back-up Procedure

1. Back-ups of the application server that hosts CPEMS are performed on a regular schedule.
2. For disaster recovery, the worst case would be a loss of data for 1 week.

System Data Output

All information printed from CPEMS is marked with a banner explaining to users the sensitivity of the data and the need for appropriate handling. If an organization needs additional wording such as local identifiers for the banner statement, the CPEMS Service Support Center can be contacted to assist with the request.



For the sake of clarity, the text of the message is presented to the right of the figure.

Figure 11: Confidentiality Warning Banner on Printed Output

Warning
This document may contain information covered under the Privacy Act. Please treat all information as confidential and therefore appropriately follow the security and confidentiality guidelines.

Physical and Environmental Protection

Physical and environmental controls are in place to protect the computing components that make up CPEMS. The CDC and NCHHSTP data centers that house CPEMS computing resources are protected with a cipher lock and card reader. All visitors must sign a visitor log when entering and exiting the computer room. The CDC & NCHHSTP Information Security Officers maintain a copy of the visitor log which includes the name of each visitor and the date and time of each visit. Physical security of the building and computer room is enhanced through the use of guards, video cameras, and surveillance equipment. All visitors must sign in at the front desk and present a positive form of identification. The guard issues a badge to each visitor, who must be escorted by a CDC employee while in the building.

Environmental controls, including temperature, humidity, sprinklers, emergency power-off switches, alarms, and uninterruptible power supplies, are used to protect CPEMS computing resources from system damage or failure.

The data centers that house CPEMS computing resources have a backup cooling system in addition to the air conditioning provided in the buildings.

The fire alarms located in the computer rooms are protected to prevent accidental triggering. A water shutoff valve is located in the computer room as well to prevent accidental triggering.

Evacuation plans and fire drills are in place and are handled at the CDC enterprise level to ensure compliance with building re-entry procedures. Additional monitors are on hand during the drills to account for CDC employees and to ensure that only authorized employees re-enter the building.

Help Desks

The DHAP IT Help Desk and CPEMS Service Support Center has been established to support CPEMS. The help desks are staffed jointly by CDC employees and contractors. The DHAP IT Help Desk will assist users with SDN, Digital Certificates and system technical issues. The CPEMS Service Support Center functions as a second tier support to answer questions about the CPEMS application. Guidance regarding the handling of an incident response in CPEMS can be found in Chapter Four.

Security Awareness Training

For CDC employees, security awareness training must be completed prior to gaining access to the CDC network. The CDC provides security awareness training programs for all employees to emphasize the importance of security to the organization. By educating employees and keeping a high level of security consciousness, the importance of preventing and avoiding many serious security breaches is emphasized. Security awareness training is mandatory and must be completed each year. If not completed, network access is disabled and the offender's reinstatement must be confirmed by a supervisor.

Security Breach Protocol

In the event CPEMS, or any CPEMS data, are breached, a reporting process is in place to report it and mitigate any deficiencies that allowed the breach to occur.

Upon the discovery of data breach, the CPEMS Security Steward or the Information System Security Officer (ISSO) should immediately be notified. The situation surrounding the breach will need to be documented, i.e. who discovered it, what data were breached, the date and time the breach occurred and any other relevant information that will be pertinent for the investigation. The steps noted below will outline exactly what needs to be documented.

Once the Security Steward has been notified, he/she will notify the Information System Security Officer (ISSO) and subsequently the CPEMS Business Steward (if he/she has not already been notified) and the Office of the Chief Information Security Officer (OCISO). If any confidential or sensitive data have been breached, the Information Security team at the Department of Health and Human Services will also need to be notified within one hour of the breach.

If confidential data are found, delete the file from the SDN folder immediately and document the following in the data extraction log:

1. Failed inspection – confidential data found
2. Type(s) of identifiers found
3. Date and time the file was deleted from the SDN server
4. Procedure followed to resolve the issue (e.g Contact names and times, any communication notes etc)
5. Immediately report any findings of confidential data to the appropriate PEB Business Steward (usually a Branch Chief), and the CPEMS Security Steward. If none of these persons are available, report directly to the Information System Security Officer.

The specific project area should be notified and conversation documented. Email notification should be sent to the site advising them of the incident and mitigation procedures should be conveyed so it does not reoccur.

Additional Security Measures for CPEMS

Data Confidentiality Protocols

External agencies as well as CDC follow certain data confidentiality protocols in order to assure the data remain protected and confidential. The Rules of Behavior (ROB), Memorandum of Understanding (MOU) and the Assurance of Confidentiality (AOC) comprise the due diligence effort that CDC and the States/Grantees follow.

The ROB covers three different personnel that are involved with CPEMS data: the CPEMS agency system administrator, and the CPEMS agency users. Each document is tailored to the particular role of the personnel that will be working the the CPEMS data. Because each role has different types of access to the data (i.e. full access, read/write role based), it is necessary to have separate ROBs in order to fully protect how CDC staff/contractors as well as CPEMS system administrators interact with the data.

An MOU exists for both CPEMS and XPEMS which defines the relationships and expectations of CDC and external States/Grantees in dealing with the data. These agreements outline how data will be protected at the CDC and the States/Grantees level using recommendations and best practices. The MOU requires a signature from management personnel at the State/Grantee organization that has decision -making authority in order to made the agreement binding.

The AOC outlines the purpose of the data and how CDC will handle data in order to prevent any identifying or sensitive information from becoming compromised and/or released to unauthorized parties both internal and external to CDC.

CHAPTER FOUR

Grantee Responsibilities

CPEMS grantee agencies that use CPEMS have responsibilities that help ensure confidentiality and security of the system and its data. The responsibilities of an agency include:

Account Management

The Agency System Administrator is responsible for managing account access for their users. The account access process includes applying for the SDN digital certificate and signing the Rules of Behavior (ROB). This is usually done in writing through a user's supervisor and should include a description of the user's duties related to CPEMS. Once a certificate is granted, the Agency System Administrator establishes an account with levels of access and permissions for that user which should only be necessary to perform their required duties. An Agency System Administrator's responsibility also includes restricting access to parts of CPEMS according to the role of the user, modifying access within the system when a user's duties change, and terminating access when employees leave, change jobs, or breach agency policies. User accounts should be reviewed yearly in order to ensure that all accounts are current. In addition, digital certificates expire yearly and must be renewed. CPEMS accounts that are inactive for two reporting periods (180 days) will be automatically disabled.

Each Agency System Administrator is accountable for their use of CPEMS and the data. Using system resources to copy, release, and view data without authorization is prohibited. Altering data improperly and tampering with the system is also prohibited. Any breaches of security, confidentiality, and unethical conduct related to CPEMS must be reported.

CPEMS Security Agreements

A survey of CPEMS users[2] revealed that, among 235 respondents, 1) the number one security issue was system vulnerability, or unauthorized access to data; and 2) that most grantees already have policies/protocols in place, to address this and other security measures.

Some of the measures in place which were listed by CPEMS users include:

- Protocols regarding securing data
- Protocols to address electronic data
- Protocols regarding staff practices
- Confidentiality of data and HIPAA compliance

[2] CPEMS User Survey of class participants, March, 2005

Data system security consists of two facets. The first is the security of the system and the second is the confidentiality of the data. The chart below explains the differences and the overlaps.

SECURITY DEFINITION	SECURITY RISKS

Maintaining the integrity of the CPEMS system to insure the existence and confidentiality of data by taking measures to detect, document and counter accidental data loss or damage; or threats to the integrity of the system	• Physical systems and facilities
	  o Acts of nature or disaster
	  o Human intruders or insiders
	• Security intrusion or system breach
	• System unavailability/ maintenance

CONFIDENTIALITY DEFINITION	**CONFIDENTIALITY RISKS**
Maintaining critical information in a confidential environment and preventing unauthorized access to sensitive data	• Autonomous intrusion (viruses/hackers) • Unauthorized access to data • Inappropriate release of data • Corruption of data • Loss of data

In an effort to provide maximum protection of the data that is entered into CPEMS, in addition to the physical and system security measures explained in this document, there are Rules of Behavior for CPEMS Agency Users (ROB-AU) regarding appropriate and allowed use of CPEMS. There are also Rules of Behavior for CPEMS Agency System Administrators (ROB-ASA) covering all of the additional duties of the Agency System Administrators. CDC also will execute a Memorandum of Understanding (MOU) with each directly funded organization. The process will work as follows:

1. Rules of Behavior for CPEMS Agency Users (ROB-AU) will be provided to each CDC directly funded organization.
    a. Each CPEMS user of the directly funded CDC grantee will sign a ROB-AU. Organizations with a CPEMS deployment model are asked not to modify or omit existing language in the ROB-AU but may add information relevant to their organization. Organizations with an XPEMS deployment model may execute the same or similar document with their users. The ROB-AUs will be retained by the CDC directly funded grantee.
    b. Each directly funded CDC grantee will also execute the same or similar document with their funded organizations to cover their users and notify the CDC when this process is complete. The ROB-AUs will be retained by the CDC directly funded grantee.
2. Rules of Behavior for CPEMS Agency System Administrators (ROB-ASA) will be provided to each directly funded organization.
    a. Each directly funded CDC organization, regardless of deployment model, will have their designated Agency System Administrator sign one ROB-ASA to attest to system administration compliance including that all users of CPEMS have signed the ROB-AU. The signed ROB-ASA will be submitted to the CDC.
    b. Each directly funded CDC grantee will be responsible to ensure that each of their funded organizations complete a ROB-ASA to document system administration

compliance. CDC will be notified by the directly funded grantee when this process is complete. The ROB-ASA should be retained by the CDC directly funded grantee.

3. Memorandum of Understanding (MOU) for CCPEMS and XPEMS
    a. For each directly funded grantee, an authorized representative who can bind the organization will sign a MOU on the use of CPEMS with CDC. The grantee organization will submit the signed MOU to the CDC.
    b. Each directly funded CDC grantee will also execute the same or similar MOU with all of their funded organizations and notify the CDC when this process is complete. The MOUs should be retained by the CDC directly funded grantee.
4. Certification of current digital certificates, accounts, and activity assignments (roles and permissions).
5. Certification that security training for all users is conducted yearly.

If you have any questions regarding these documents, please see your CPEMS regional lead or call the CPEMS Service Support Center.

These documents are explained in the following table.

DOCUMENT	DEFINITION	HOW EXECUTED
Rules of Behavior, CPEMS Agency Users	Generally, Rules of Behavior dictate an individual's responsibilities as a system user, and provide guidelines and policies surrounding what is and what is not acceptable system behavior. Specifically, the CPEMS Rules of Behavior provide system users with information about controlling hardware, and managing system access including granting and revoking privileges, controlling data, and managing personnel, among other things. The contents are defined by the NIST guidelines. This is required by the System Authorization process.	• Between CDC and directly funded grantees • Between grantees and their users
Rules of Behavior, CPEMS Agency System Administrators	Rules of Behavior that dictate Agency System Administrator responsibilities and provide guidelines and policies surrounding what is and what is not acceptable Agency System Administrator behavior with regard to CPEMS. The contents are defined by the NIST guidelines. This is required by the System Authorization process.	• Between CDC and directly funded grantee Agency System Administrators • Between CDC grantees and their grantee Agency System Administrators
MOU, CCPEMS	This is a written document which establishes policies or procedures of mutual concern to CDC and CPEMS users. It provides a general description of the responsibilities that are to be assumed by each party in pursuit of some goal or goals. It is not a contract. It is used to define areas of mutual interest. This is required by the System Authorization process.	• Between CDC and CCPEMS user organizations • Between CCPEMS users and their agencies

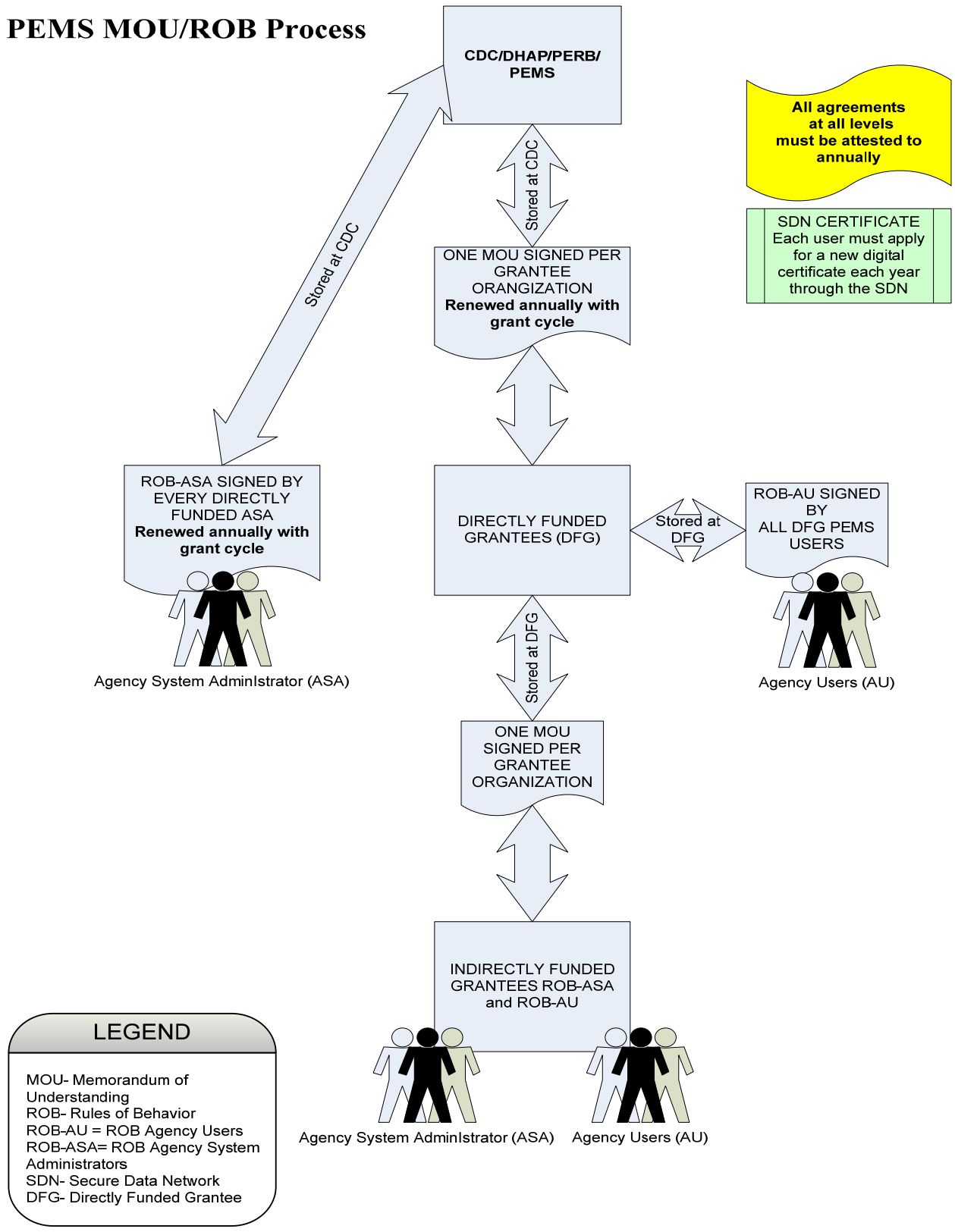


Figure 12: CPEMS MOU/ROB Process

Incident Response

Detect the Incident

The key to incident response is the ability of the Incident Reporter to distinguish between an incident and a routine event. Common indications of an incident include the following:

- Antivirus software detects a host infected with a worm
- Intrusion Detection System identifies Phishing, SPAM, Spyware other malicious code
- Web server crashes
- Users complain of slow access to hosts on the Internet or Intranet
- Agency System Administrator sees a filename with unusual characters
- Host records an auditing configuration change in its log
- Logs increase in size in shorter than usual timeframes
- Logs show multiple failed login attempts from an unfamiliar remote system.

There are many such indications; therefore this list is not exhaustive. Furthermore, some of these indications may turn out to be benign events. For example, slow connection speeds may be due to a faulty modem or network card, or problems at the local ISP. Multiple failed login attempts may be the result of a user having forgotten his or her password and trying repeatedly to guess it. On the other hand, a defaced Web page is very clearly an indication that an incident has occurred.

First Response for CPEMS Agency System Administrators

The role of an Agency System Administrator is vital in ensuring all aspects of network security and maintenance. This individual also plays the most important role in the event a computer is used in a security incident or unlawful act. The Agency System Administrator will be the primary point of contact for individuals that need to make a report of computer use violations. In addition, an Agency System Administrator may come across a violation during the normal course of their duties. The actions taken by the Agency System Administrator after discovery of a potential computer violation will play a vital role in the investigation, forensic evaluation of the computer system, and potential prosecution or administrative actions. From a forensic standpoint, the ideal situation is to isolate the computer from additional use or tampering.

In the event of a suspected computer incident, great care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, merely opening a file changes it. In a legal sense, it is no longer the original evidence and at that point may be inadmissible as evidence. Opening a file also alters the time and date it was last accessed. No attempts should be made to recover or view files except by qualified IT professionals.

Once it is determined that an incident is occurring (or has occurred) or could possibly be occurring, appropriate personnel should be notified immediately. At this point in the process, making the appropriate contact, and only the appropriate contact, is critical.

The hierarchy of notice regarding a suspected or determined incident in CPEMS is as follows:

1. CPEMS User (also known as Incident Reporter) reports suspected incident to Agency System Administrator (who will help determine if an incident has occurred)
2. Agency System Administrator reports to Local IT staff (who will determine, if possible, what occurred; what should be done about it; and what should be investigated or reported further)
3. Local IT staff notifies DHAP IT Help Desk, if necessary
4. DHAP IT Help Desk notifies the ISSO, if necessary
5. ISSO informs OCISO, if necessary.

Training

All agency staff dealing with CPEMS data should be trained on policies and procedures established by the agency, the legal aspects of data collection, and the ethics of their responsibility to the clients. Training should cover state regulations and the agency's policies concerning confidentiality, computer security, and legal obligations under non-disclosure agreements. Grantee staff should be aware of common threats to confidentiality and security, contingency plans for breaches of confidentiality and security, and the penalties associated with breaches of confidentiality and security. Each agency staff member with access to CPEMS data should receive CPEMS training including security updates.

Security Recommendations for Your Grantee Agency

Grantees are expected to have written security and confidentiality policies and procedures to protect their data. Here is a checklist of items that grantees should consider when writing policies and procedures regarding the secure and confidential implementation of CPEMS at their agency.

Accountability

Users of the CPEMS system should be held accountable for their use of the system and its data. Using system resources to copy, release, or view data without authorization is prohibited. Altering data improperly or otherwise tampering with the system is prohibited. Employees authorized to access client-specific data are responsible for the protection of confidential information and must report any breaches.

Administration of Proxies

CPEMS provides the ability to identify and assign proxies, i.e., the ability to assign one person's permissions to someone else. Although multiple users can be granted proxies for an individual, only one user can log in at a time, as a proxy of another user. Only an administrator has permission to grant and delete a proxy. Rules should be developed at the site level to determine how long proxies may last and how they should be administered. All users will comply with the rules of proxy administration.

Grantee Responsibility

Each agency directly funded by CDC should identify a person with the ultimate responsibility for the CPEMS system. This person will sign the MOU with CDC and maintain the terms of the agreement with agencies they fund with CDC grant money. In addition, agencies must maintain ROB agreements with users who directly access the system. Agencies must submit signed copies of system agreements to CDC. Certification of current certificates, accounts, and activity assignments must be done, and annual security training for the system must be completed.

Backing-Up Data

CDC regularly backs up all CPEMS data stored on CDC database servers. CPEMS data that are not yet transmitted, either because they have not yet been entered in the system or because the data are not being stored on CDC servers (XPEMS) must be backed up periodically by the grantee. Frequency of backup should depend upon how often the data changes and how significant those changes are, but should be done based on a fixed schedule that is part of the normal maintenance of the system. Backup copies should be tested to make sure they are actually usable and stored under lock and key in a secure area and a separate copy of data kept at a secure off-site location if possible.

Breaches of Confidentiality

A breach of confidentiality is any failure to follow confidentiality protocols, whether or not information is actually released. This includes a security infraction that results in the release of private information, with or without harm to one or more individuals. All suspected breaches of confidentiality or security (e.g., possible viruses, hackers, password divulgence, lost or misplaced storage media) should be reported immediately to the CPEMS Agency System Administrator. This administrator will determine the cause, develop and implement process improvements and/or determine if the incident should be reported to the CPEMS Security Coordinator via the CPEMS Service Support Center.

At the local level, sanctions for violations of confidentiality protocols should be established in writing, as part of the organizational policies and should be consistently enforced.

Controlling Access to CPEMS

Access to CPEMS files and software must be restricted to authorized users. Usually this involves establishing user accounts, limiting activities within the system, and terminating access when employees leave, change jobs, or breach agency policies. Typically, those assigned duties that require access to CPEMS software or data, must be granted those privileges by the CPEMS Agency System Administrator. Ideally, this process should come through the user's supervisor as a documented request. The request should include a description of the user's duties related to CPEMS. The CPEMS Agency System Administrator can then establish an account for the user, specifying permissions and levels of access the user will have (which should only be those sufficient to perform the duties required by the job). General training regarding security and confidentiality is also recommended.

Controlling and Protecting Data

CPEMS-related data do not exist on CPEMS servers alone. Such data may exist on collection forms, counselor notes, floppy disks, CD-ROM drive and other information storage media. Use of dial-up access, modem for data collection activities, or working from home with CPEMS data should be prohibited or restricted to specifically authorized personnel working under carefully defined circumstances only. Since all these media may contain confidential information, the agency must develop policies and procedures for the use, storage, and disposal of all media used to record or store CPEMS data. Following is a list of good security practices and safeguards to protect data. This list is not exhaustive, but should serve as a guide to good practices.

- Keep records locked at all times
- Keep disks, laptops, thumb drives locked
- Use disk encryption on laptops and encrypted thumb drives
- Lock your room and know who has the keys
- NEVER give data to anyone for any purpose without a signed agreement regarding its use
- Know to whom you gave confidential records
- “Just say no” if someone gives you something you shouldn’t or don’t want to see
- Do not send Information in Personnally Identifiable Information (PII) by email, fax or other less secure means to the CDC or to other organizations with whom you collaborate
- Don’t keep private information that you don’t need to do your job
- Don’t keep CPEMS data on a laptop or at home
- Clear out web browser sessions, even at work
- Do not install instant messaging on any computer containing CPEMS data
- Do not check personal webmail accounts from work
- Do not open any attachments sent by an unknown party

Controlling Personnel

Personnel are as much a part of a data collection and reporting system as computer hardware and collection forms. People are usually the weakest link in any security system. All personnel dealing with CPEMS data should be trained on the policies and procedures established by the agency, the legal aspects of the data collection, and the ethics of their responsibility to the clients. Furthermore, they should also be aware of the penalties associated with breaches of confidentiality or security. Each agency should have a policy on confidentiality and security. The confidentiality and security policy must make clear that authorized users are responsible for knowing the confidentiality and security policies and procedures, challenging unauthorized users, reporting possible breaches, and protecting equipment and data. Staff should be required to sign a statement acknowledging that they have been made aware of the confidentiality and security requirements for the agency. The signed statement should be kept in the employee’s file.

Encryption

CPEMS data are sensitive, confidential information that may have legal and personal implications for clients; therefore, it should be protected from unauthorized access. Data transmitted to CDC through the SDN is secured through the use of all security controls described in this document. An encrypted tunnel is established for the transport of the data from the State/Grantee site to CDC.

If an organization decides to send data to anyone other than CDC, the data should be encrypted. All CPEMS data are encrypted using the Self Decrypting Archive function of PGP. An encrypted SDA file is generated using PGP, then sent to CDC over the SDN. This approach employes a multi-layer encryption technique using the latest encryption technology to ensure the data is secure. The data remain encrypted until entering the CDC network and reaching the validation team at which time the data are decrypted. PGP meets the Federal Information Processing Standards 140-2 (FIPS 140-2) for encryption requirements as well as the CDC central key management requirement for CDC by the Chief Information Security Officer.

Levels of Access

Many users are unlikely to need access to all parts of CPEMS. Access to the various components of the system should be restricted based upon the user's role. For example, typical roles include data entry, generating reports, system administration, and viewing information. Some users may need to read information about clients but not enter data. Users should maintain the rights to only the systems that they need, and only for the time that they need them. The CPEMS Agency System Administrator should develop a security policy that allows for appropriate access rights for individuals based on their assigned roles within CPEMS.

Locking Workstations

All users should secure their workstations before leaving them. Automatic screen saver locks should also be set to engage whenever the system is left idle (15 minutes of inactivity). In order to unlock the screensaver, the system should require entry of the user's ID and password.

Physical Security of Equipment

CPEMS Agency System Administrators should maintain an inventory of all system hardware and software provided to system users, and periodic audits should be conducted to account for all assets. Visitors or unauthorized personnel should not be allowed unescorted access to areas containing computers holding CPEMS data All computer equipment should be protected by surge suppressors and emergency battery power to prevent data loss in case of fluctuations in the power supply. All computers and other equipment used for CPEMS should be housed or stored in secure areas and physically attached to an immovable object, if possible. All rooms where CPEMS data are stored, either on paper, computer or other storage media should be locked at all times when not in use and it should be known with whom the keys reside.

Records Disposal

Many states have laws or regulations concerning how long client records must be stored, and when and how they must be destroyed. Agencies must develop policies and procedures that comply with these state regulations. When client records are to be destroyed, this should include not only paper records but also electronic records. Please note that "deleting" a file or record on the computer does not actually remove the information from the system. Even overwriting or formatting the media may not sanitize it; special sanitization programs or physical destruction of the storage media may be required. Agencies must be sure to sanitize or destroy hard drives of computers scheduled for disposal or transfer to staff not authorized to use CPEMS.

Release of Data

Agencies must develop a written policy and procedure for releasing data. These policies should be periodically reviewed and modified to improve the protection of confidential information. Policies concerning the release of de-identified and aggregate data that prevent indirectly identifying clients through small denominators should also be established. Access to any data containing confidential information or case-specific data should be contingent on having a signed, current, binding non-disclosure agreement currently on file at the individual agency. These agreements must include discussion of possible employee ramifications and criminal and civil liabilities for unauthorized disclosure of information.

Releasing Data to Partners

In order to assist other agencies in tracking referrals or other related purposes, agencies may enter into agreements with other agencies to share limited information about specific clients. Data sharing should be based upon written agreements and clients should be helped to understand how their confidential information will be treated/shared with other agency partners. Agencies must develop policies and procedures to comply with state regulations regarding release of data.

Releasing Data to the Public

Except under conditions specified in writing and explained to clients, only authorized staff members who have signed a binding non-disclosure agreement (and who have a need to know) should be allowed access to sensitive client identifying data. Agencies should have a policy and protocol for releasing de-identified and aggregate data for use in analysis, grant applications, reporting and administrative functions. This policy should specify what data may be released, in what form, to whom the data may be released, and who may approve the release of data.

Reporting to CDC

Reporting to CDC should be done according to the schedule specified by CDC. While data may be entered in to CPEMS at any time, data are not reported to CDC until the appropriate files are submitted to CDC by the authorized personnel of each agency over the SDN. There should be policies and procedures developed to specify the data quality assurance process that should be implemented and the administrative approval process that should be followed prior to reporting/submitting data to CDC.

Storage Media

Agencies should establish policies and procedures that outline when it is appropriate to export CPEMS data to storage media. All storage media should be clearly labeled. Removable media such as CD or DVD disks, etc., should be destroyed or sanitized with disk wiping tools before reuse or disposal. Storage media, whether removable or fixed, paper or electronic, containing CPEMS data should be stored in a secured area. Data removed from secured areas for analysis should be de-identified first. Disks, laptops, thumb drives and other storage media that contain CPEMS data should have only the minimum data necessary to perform a given task; should be encrypted or stored under lock and key when not in use; and (except for backups) be sanitized immediately following the task completion. Cleaning crews, maintenance staff, and other unauthorized personnel must be escorted into secured areas by designated staff. Encryption of data during storage is recommended.

Terminating Access

As soon as individuals change duties within an agency or leave the agency altogether, their access privileges should be modified. As part of the transition or departure procedures, the Agency System Administrator should be notified of changes to employment status so the proper actions can be taken to protect the system and its data.

Training on Confidentiality

Each staff member with access to CPEMS data must receive training on confidentiality and security. Training should cover the state regulations concerning confidentiality, the basics of computer security, the agency's confidentiality and security policies and procedures, the roles and responsibilities of various staff positions regarding protecting confidentiality and security, contingency plans for breaches of confidentiality or security, common threats to confidentiality and security, legal obligations under non-disclosure agreements, and potential effects on clients and the agency to breaches of confidentiality.

Unauthorized System Intrusion

Any computer with external connectivity (especially one connected to the Internet) is subject to unauthorized penetration from hackers, computer viruses and worms. Agencies must take all reasonable precautions to protect their systems from intrusion. A plan must be developed and implemented to prevent and, if necessary, recover from changes to the system caused by unauthorized access. Typical precautions include using effective passwords, installing

firewalls and anti-virus software, making backup copies of the data at regular intervals so that the system can be restored to a previous state, making shredding equipment available, and training staff in basic computer security such as password confidentiality, and the risks of unauthorized installation of software.

Use of Equipment

The computers, servers, and other electronic equipment used to collect, enter, copy, store, analyze, or report CPEMS data should be under the control of the agency. The use of equipment related to CPEMS, including Internet connections, e-mail, photocopiers, facsimile machines, and other equipment that might be used to copy, transmit, or process CPEMS data should be regulated by written policies and procedures. These policies should require personnel to electronically lock unattended computers, and ensure that computers have screensaver locks that are activated after 15 minutes (or less) of inactivity.

Use of Passwords

Passwords must be used to confirm the user identity. Passwords should be changed periodically (at least every 90 days) and staff should be cautioned not to share passwords. The CPEMS application will lock-out a user after three consecutive unsuccessful log-in attempts. De-identified databases should be held securely (e.g., password protected) until authorized for public use. Similar security measures should be incorporated into the operating system user policy.

Use of Portable Equipment

While the use of portable computers has its advantages, it also creates additional security risks, such as loss or theft of the computer and data it stores. If computers are used outside the office, agencies should establish policies regarding physical security (the computer should be locked to an immovable object), and digital security (the computer should be protected with a unique username, complex password, and sensitive data should be encrypted). Laptop computers and other portable hardware that receive CPEMS data should store that data in encrypted formats. Laptops should employ whole disk encryption in order to protect any sensitive data that may be stored on the hard drive.

GLOSSARY

Term	Definition
Access control	A set of procedures intended to assure that a person is who he or she claims to be and has been authorized to perform a set of functions or access a dataset.
Aggregated data	Information, usually summary statistics that may be compiled from personal information, but is grouped to prevent the identification of any individual case.
Assurance of confidentiality	An assurance that identifying information (confidential data with and without identifying information) will be held in strict confidence, will be used only for the stated purposes, and will not otherwise be disclosed or released without the consent of the individual.
Authorized access	The permission granted to individuals to see full or partial data that could be linked to an individual.
Authorized personnel	The individuals employed by the grantee who, in order to carry out their duties, have been granted access to confidential data. Authorized personnel must have a current, signed, approved, and binding non-disclosure agreement on file.
Breach of data security	Any unauthorized use of data, even data without names, intended or unintended, including failure to follow security protocols, even if no data are released.
Breach of confidentiality	A security infraction that results in the release of private information, with or without harm to one or more individuals.
Case-specific information	Any combination of data elements that could identify a person.
Certificate of Confidentiality	A guarantee that identifying information (confidential data with and without identifying information) will be held in strict confidence, will be used only for the stated purposes, and will not otherwise be disclosed or released without the consent of the individual.
Confidential information	Any information about an identifiable person when the person or establishment providing the data or described in it has NOT given consent to make the information public
Confidentiality	The protection of private information collected for the system.
Confidential record	A record containing private information about an individual or establishment.
De-identified	The removal of personal data (e.g., names, addresses, ZIP codes, and telephone numbers) so that a record cannot be linked to an individual, but still allows the remaining data to be analyzed.
Encryption	The manipulation or encoding of information so that only parties intended to view the information can do so.
Management controls	Controls that include policies for the operation of information

Term	Definition
	technology resources and for authorizing the collection, processing, storage, and transmission of information. These controls may also include the training of staff, oversight, and appropriate response to infractions.
Personal identifier	A datum, or collection of data, that allows the possessor to determine the identity of an individual with a specified degree of certainty. A personal identifier may permit the identification of an individual within a database (e.g., client code number).
Personnel controls	Staff member controls such as training, separation of duties, background checks, etc.
Physical controls	Controls using barriers, such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc.
Quality assurance	Activities to enhance or maintain performance levels of a process; usually involves measurement of the current level of performance, development of methods to maintain or improve that level, and implementation of those methods.
Records retention policy	Assigning a length of time records must be maintained and a date at which paper or electronic records should be archived or destroyed.
Role-based access	Access to specific information or data granted or denied based on the user's job status or authority. Roles typically group users by their work function. This control mechanism protects data and system integrity by preventing access to unauthorized applications and data. Defining access based on roles within an organization, rather than by individual users, simplifies an organization's security procedures.
Sanitize	Also known as disk-wiping, sanitizing is the act of completely destroying the information on a hard disk, CD, DVD, or other storage media to ensure that all traces of the files are unrecoverable.
Secured area	A physically contained area where confidential data are available. Only authorized staff members have access to this area. The secured area is usually defined by a hard, floor-to-ceiling wall with a locking door and may include other measures (e.g., alarms, security personnel).
Security	The protection of data and information systems, with the purpose of preventing unauthorized release of identifying information (e.g., preventing a breach of confidentially) and protecting the integrity of the data by preventing accidental data loss or damage to the systems.
Technical access controls	Controls involving technology, such as requirements for password use and change.

REFERENCES

Document Name	Document Title
NIST Special Publication 800-12	An Introduction to Computer Security: The NIST Handbook
NIST Special Publication 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST Special Publication 800-18	Guide for Developing Security Plans for Information Technology Systems
NIST Special Publication 800-30	Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology
NIST Special Publication 800-34	Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology
NIST Special Publication 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems
NIST Special Publication 800-53 Rev 2	Recommended Security Controls for Federal Information Systems
NIST Special Publication 800-59	Guideline for Identifying an Information System as a National Security System
NIST Special Publication 800-60 v1	Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
NIST Special Publication 800-60 v2	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
CDC Information Security Policy	CDC Information Security Policy
CDC Standard Policy	A Set of Standard Policies at CDC
CDC/ATSDR Policy on Releasing and Sharing Data	CDC/ATSDR Policy on Releasing and Sharing Data
CDC Information Resources Management, Protection of Information Resources	CDC Information Resources Management, Protection of Information Resources
HHS Automated Information Systems Security Program Handbook	HHS Automated Information Systems Security Program Handbook
HHS Baseline Security Requirements Guide	Information Technology Security Program: Baseline Security Requirements Guide
FIPS 46-3	Data Encryption Standard (DES)
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 197	Announcing the Advanced Encryption Standard (AES)
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
Guidelines for HIV/AIDS Surveillance	Appendix C: Security and Confidentiality

Document Name	Document Title
OMB Appendix A	Rules of Behavior
CPEMS Evaluation Guidance Data Collection Training Facilitators Handbook	CPEMS Evaluation Guidance Data Collection Training Facilitators Handbook
Technical Guidance for HIV/AIDS Surveillance Programs, Volume III	Security and Confidentiality Guidelines